MDaemon®
Email Server
This program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program or any portion of it, may result in severe criminal and civil penalties, and will be prosecuted to the maximum extent possible under law.
Copyright 1996-2008 Alt-N Technologies, Ltd.

Fare troubleshooting e rintracciare le email con i log di MDaemon

Claudio Panerai - Direttore Tecnico di Achab S.r.l.
claudio.panerai@achab.it

Troubleshooting di MDaemon:

- Problemi ricorrenti
- Come procedere
- Strumenti di analisi
- Esempi

Problemi ricorrenti

- Non riesco a inviare una e-mail a ...
- Non riesco a inviare ...
- Non riesco a ricevere una e-mail da ...
- Non riesco a ricevere ...
- Ricevo e-mail duplicate ...
- Le code sono bloccate ...
- Il server è finito in black list ...
- Trovo un winsock error nei log ...
- Falsi positivi/negativi nello spam ...

Problemi ricorrenti – possibili cause (I)

non riesco a inviare una email a ...

- L'indirizzo di email è errato
- Il server di destinazione risponde con un errore temporaneo (es. greylisting)
- Il server di destinazione rifiuta il messaggio
- Errori di timeout

non riesco a inviare ...

- Servizio SMTP fermo/conflitto con IIS
- La coda remota è bloccata
- Il provider rifiuta l'inoltro da parte di un server di posta (es. 191.mail.biz di Telecom)
- Il provider richiede l'autenticazione singola
- Firewall/Proxy SMTP che bloccano il traffico
- L'IP è in blacklist
- Socket error

Problemi ricorrenti – possibili cause (II)

non riesco a ricevere da ...

- Uno dei controlli in ingresso fallisce e cancella o rifiuta il messaggio
- Regole di filtro contenuti che cancellano/deviano il messaggio
- Inoltri con cancellazione del messaggio nella mailbox

non riesco a ricevere ...

- Conflitti con antivirus (es. Multipop e servizio IMON di Nod32)
- Troppe sessioni POP3 contemporanee verso lo stesso provider
- Mailbox piena (quote)

Problemi ricorrenti – possibili cause (III)

ricevo email duplicate

- Ricezione in domainPOP
- Sessioni POP incomplete
- Errato utilizzo dei forward
- La sessione SMTP-IN non termina correttamente

Le code sono bloccate

- Messaggio bloccante
- Errori aggiornamento antivirus
- Database del filtro bayesiano troppo grande
- Conflitti con antivirus

Problemi ricorrenti – possibili cause (IV)

Server finito in blacklist

Perché si finisce in blacklist?

Le cause possono essere molteplici:

- Il server di posta è un open relay
- Il server di posta consente il relay a nome di postmaster, abuse, webmaster, info senza che sia richiesta l'autenticazione
- Il mail server è infetto da un mass mailing virus, or some sort of spam sending compromise (open proxy, trojan, spambot, insecure AnalogX/wingate etc)

Problemi ricorrenti – possibili cause (V)

Winsock error nei log

- (10048) Conflitto con altre applicazioni su un determinato servizio (es. 2 servizi SMTP sulla porta 25
- (10049) Tentativo di aprire dei socket su IP che non appartengono alla macchina.
- (10061) Problemi di connessione con l'host remoto, ad esempio se si tenta di connettersi ad un servizio inattivo oppure se l'ISP blocca il traffico SMTP in uscita

Lista dettagliata (in lingua inglese) delle varie tipologie di errori Winsock:
http://www.altn.com/Support/KnowledgeBase/KnowledgeBaseResults/?Number=KBA-01196

Problemi ricorrenti – possibili cause (VI)

Falsi positivi / negativi nello SPAM

- Modifiche alla configurazione (es. disabilitazione DNSBL dopo update alla 10)
- Modifiche alle regole e punteggi spamassassin (update)
- Autenticazione SMTP non richiesta (anche per utenti locali)
- Problemi con URIBL
- Mancato utilizzo delle tecnologie più recenti (SPF, DKIM, ...)
- Errato utilizzo delle white list

Come procedere

Come si procede per analizzare un problema?

1. Verificare se il problema è già noto (ed è già disponibile la soluzione)
   - Knowledge base di Achab/Alt-N
   - Forum Alt-N
   - Google
2. Analizzare il problema
   - File di log di Mdaemon
   - Prompt dei comandi di Windows
   - Backup della configurazione di Mdaemon.
   - Tool on-line di diagnostica:
   - Gestione Code di Mdaemon
3. Contattare supporto Achab

Verificare se il problema è già noto

Knowledge Base di Achab

http://www.achab.it/kb

Esempi:

- **KB50541** - Non riesco ad inviare posta da MDaemon utilizzando un servizio SMTP fornito da Telecom. Configurando Outlook o Outlook Express per utilizzare questo servizio l'invio funziona, ma da MDaemon ottengo un errore 501 "*bad address*"
- **KB50374** - In una sessione SMTP in ingresso la verifica sulle DNS-BL configurate sembra fallire e trovo nei log di MDaemon il seguente errore:
  "'Recipient unknown' given and connection dropped to divert future spam"

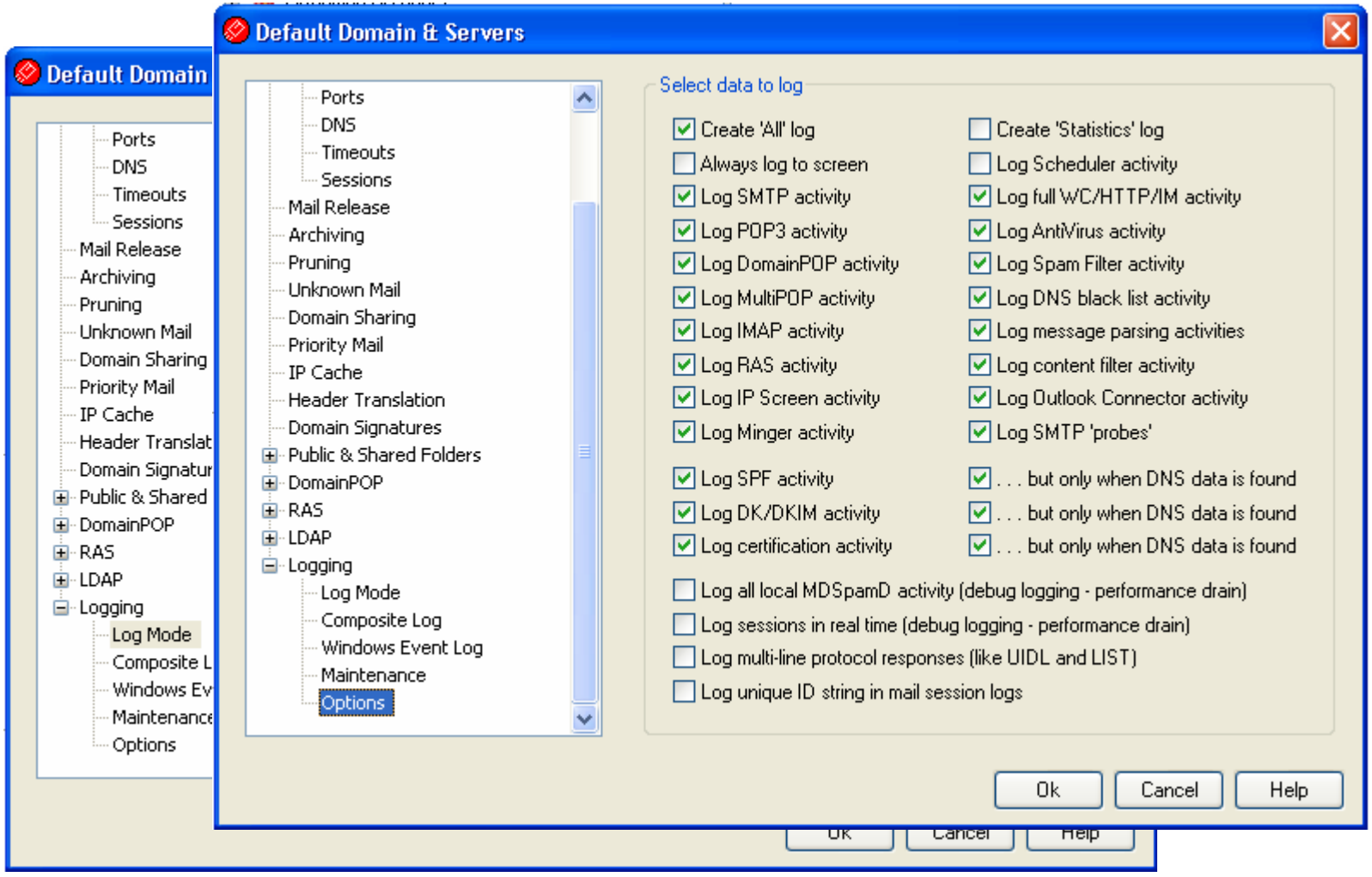
Knowledge Base di Alt-N

http://www.altn.com/Support/KnowledgeBase/

Forum di Alt-N

http://www.altn.com/Support/CommunityForums/

Strumenti di analisi – File di log (I)



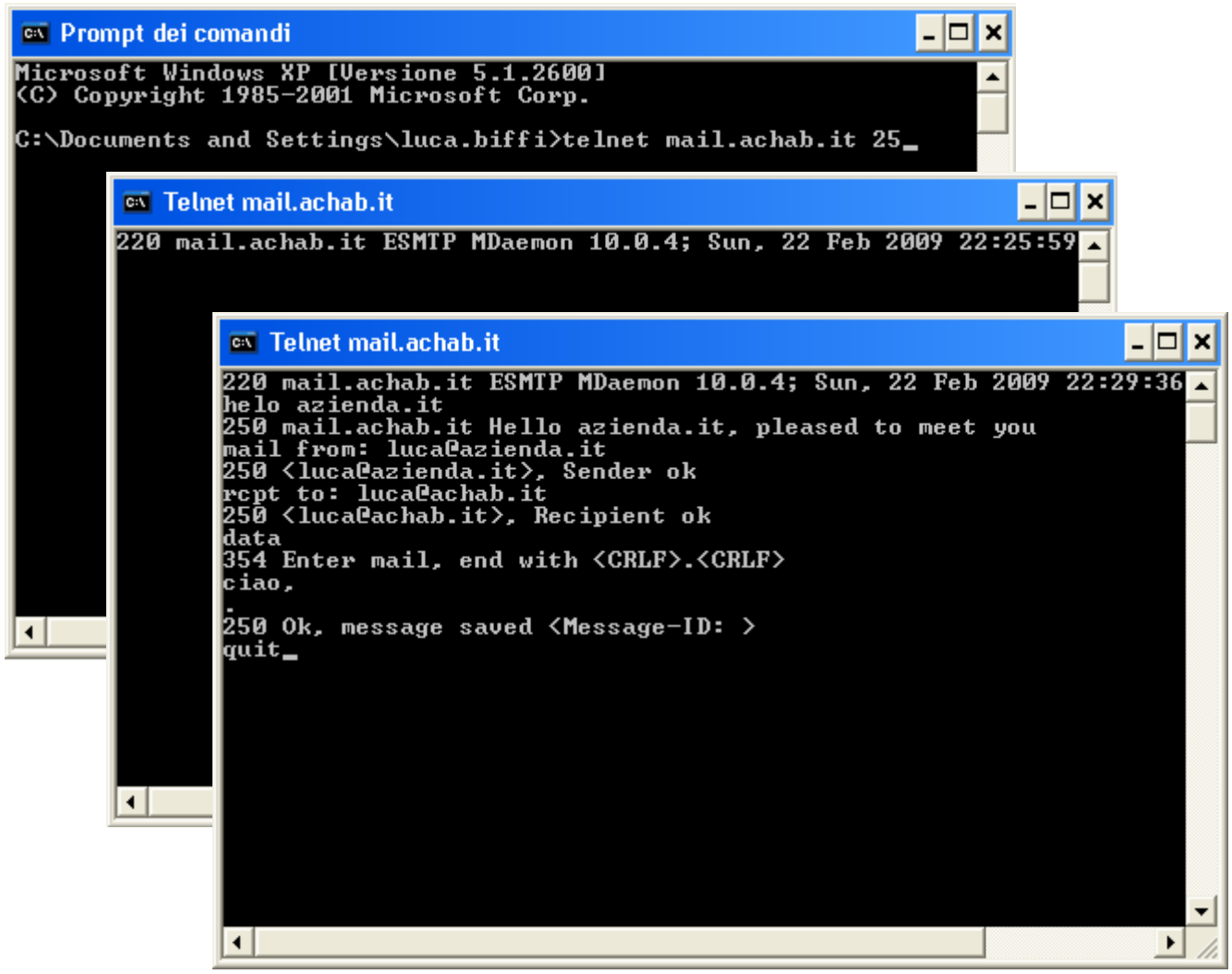
Strumenti di analisi – File di log (II)

- Servono per seguire passo passo cosa succede all'interno di Mdaemon
- Per effettuare il debug è necessario abilitare determinati tipi di log:

KB50568 - Quali sono le impostazioni raccomandate per i log in MDaemon?

- **Attenzione alle prestazioni** (lentezza e spazio disco):
  KB50565 - Come posso migliorare le prestazioni di MDaemon?

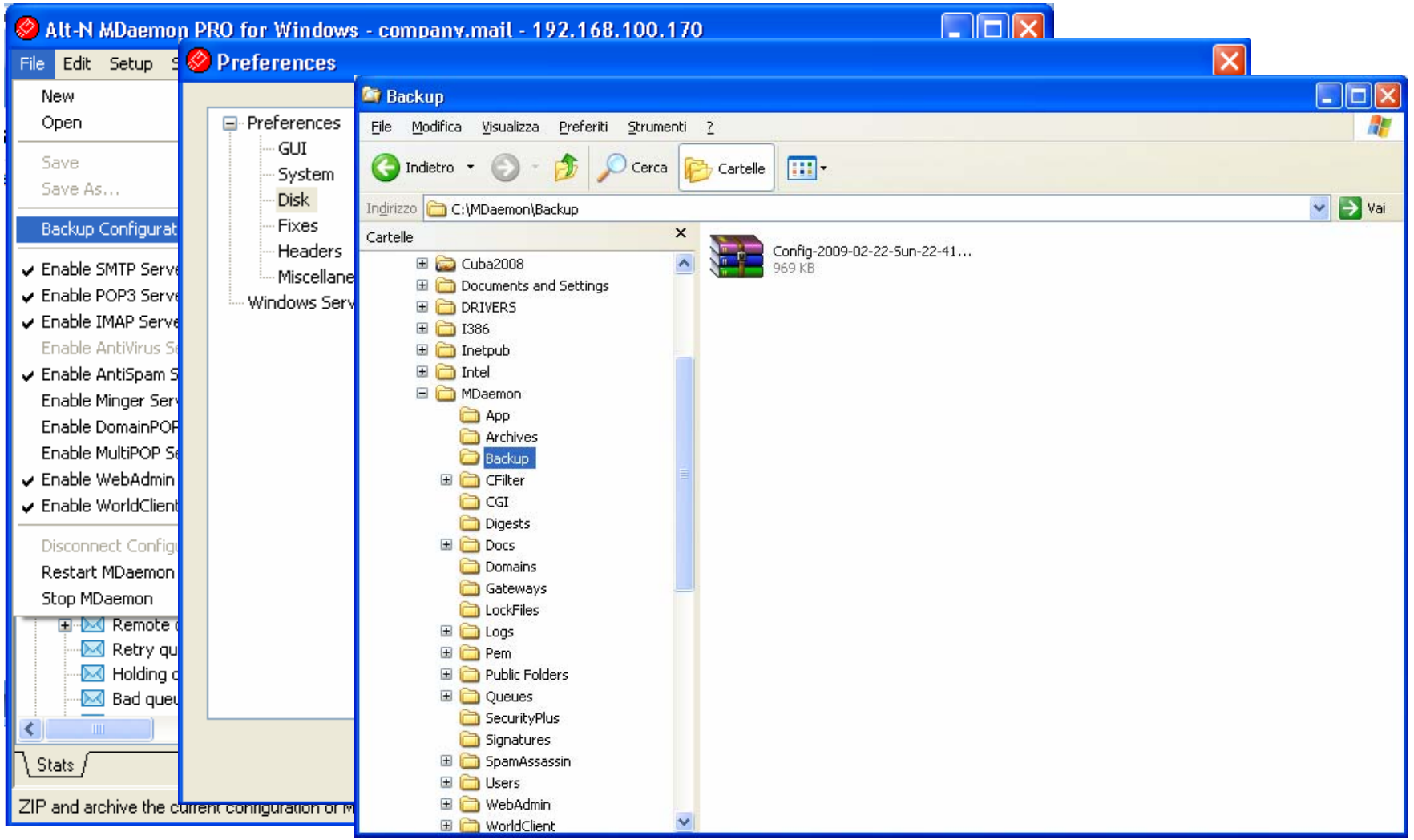
Strumenti di analisi – Prompt dei comandi (I)


Prompt dei comandi
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\luca.biffi>telnet mail.achab.it 25
Telnet mail.achab.it
220 mail.achab.it ESMTP MDaemon 10.0.4; Sun, 22 Feb 2009 22:25:59
Telnet mail.achab.it
220 mail.achab.it ESMTP MDaemon 10.0.4; Sun, 22 Feb 2009 22:29:36
helo azienda.it
250 mail.achab.it Hello azienda.it, pleased to meet you
mail from: luca@azienda.it
250 <luca@azienda.it>, Sender ok
rcpt to: luca@achab.it
250 <luca@achab.it>, Recipient ok
data
354 Enter mail, end with <CRLF>.<CRLF>
ciao,
.
250 Ok, message saved <Message-ID: >
quit

Strumenti di analisi – Prompt dei comandi (II)

- Verificare la connettività ad un server di posta
- Verificare quale servizio risponde su una determinata porta (conflitto Mdaemon/IIS)
- Testare l'invio di un messaggio in SMTP dal server Mdaemon: **KB50488** - Utilizzare una session telnet per testare l'invio di un messaggio
- Testare la ricezione POP3 (MultiPOP/DomainPOP) sul server MDaemon

Strumenti di analisi – Backup della configurazione (I)



Strumenti di analisi – Backup della configurazione (II)

- Debug di problemi complessi che dipendono dalla combinazione di configurazioni
- **Attenzione** ai servizi attivi

Strumenti di analisi – Tool di diagnostica

- **Network tools** (free):

  http://www.network-tools.com

  validazione email, dati DNS, reverse lookup, …
- **DNS Stuff** (pagamento):

  http://www.dnsstuff.com

  tutti i tipi di test
- **Open DNS** (free):

  http://www.opendns.com

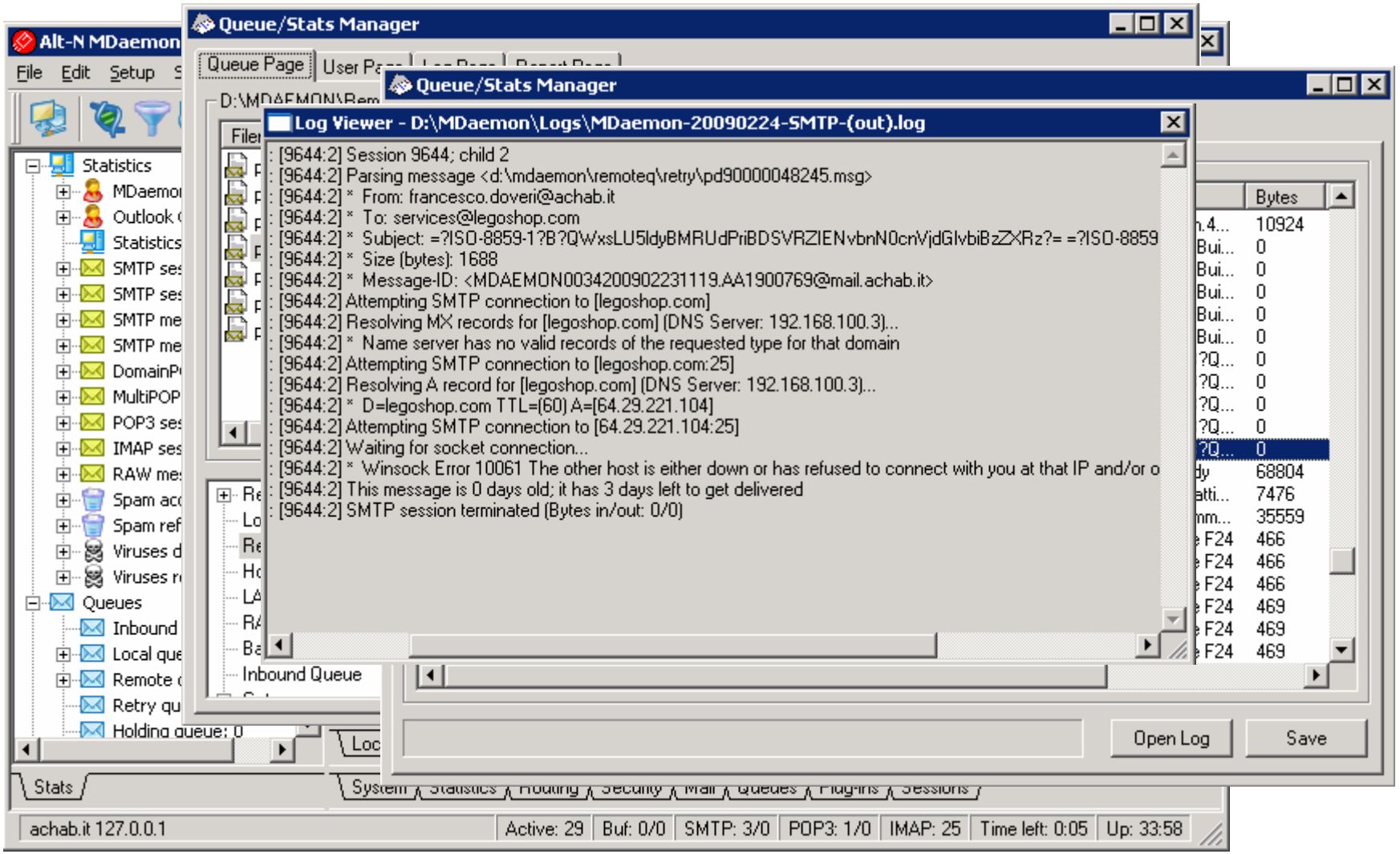
  DNS temporanei. Altri:195.20.105.149 e 213.133.115.5
- **DNSBL** (free):

  http://www.spamhaus.org

  http://www.spamcop.net

  verifica se il proprio IP è listato (in varie black list)

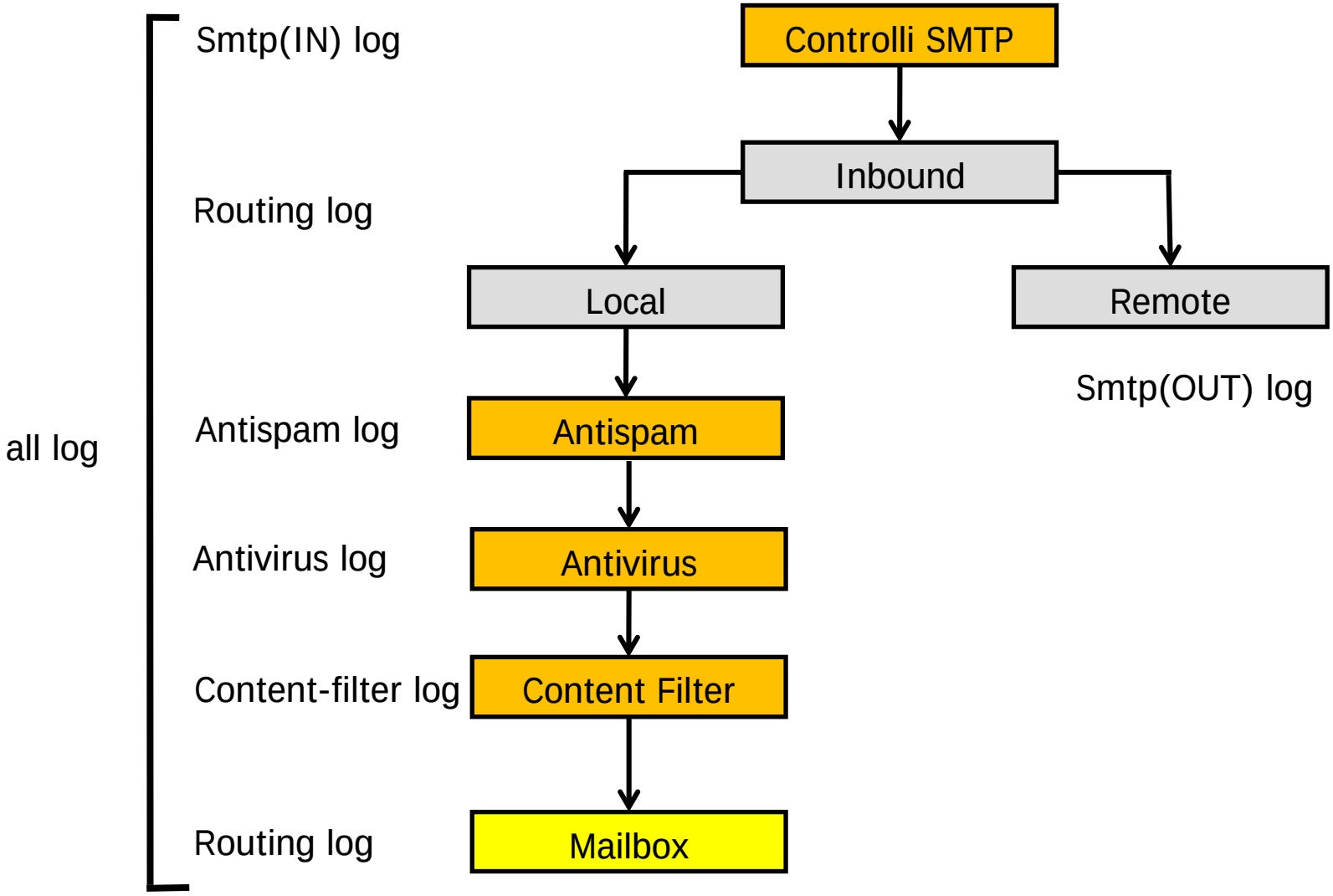
Strumenti di analisi – Gestione code di Mdaemon (I)


Queue/Stats Manager
Queue Page
Log Viewer - D:\MDaemon\Logs\MDaemon-20090224-SMTP-(out).log
: [9644:2] Session 9644; child 2
: [9644:2] Parsing message <d:\mdaemon\remoteq\retry\pd90000048245.msg>
: [9644:2] * From: francesco.doveri@achab.it
: [9644:2] * To: services@legoshop.com
: [9644:2] * Subject: =?ISO-8859-1?B?QWxsLU5ldyBMRUdPcriBDSVRZIENvbnN0cnVjdGlvbiBzZXRz?= =?ISO-8859
: [9644:2] * Size (bytes): 1688
: [9644:2] * Message-ID: <MDAEMON0034200902231119.AA1900769@mail.achab.it>
: [9644:2] Attempting SMTP connection to [legoshop.com]
: [9644:2] Resolving MX records for [legoshop.com] (DNS Server: 192.168.100.3)...
: [9644:2] * Name server has no valid records of the requested type for that domain
: [9644:2] Attempting SMTP connection to [legoshop.com:25]
: [9644:2] Resolving A record for [legoshop.com] (DNS Server: 192.168.100.3)...
: [9644:2] * D=legoshop.com TTL=(60) A=[64.29.221.104]
: [9644:2] Attempting SMTP connection to [64.29.221.104:25]
: [9644:2] Waiting for socket connection...
: [9644:2] * Winsock Error 10061 The other host is either down or has refused to connect with you at that IP and/or o
: [9644:2] This message is 0 days old; it has 3 days left to get delivered
: [9644:2] SMTP session terminated (Bytes in/out: 0/0)
Open Log
Save
achab.it 127.0.0.1
Active: 29
Buf: 0/0
SMTP: 3/0
POP3: 1/0
IMAP: 25
Time left: 0:05
Up: 33:58

Strumenti di analisi – Gestione code di Mdaemon (II)

- Muovere i messaggi da una coda all'altro in modo sicuro
- Parsing veloce dei file di log
- Visualizzazione dettagli sessioni
- Esportazione dati cumulativi (integrazione con altri applicativi)

Esempi - Problemi di ricezione (SMTP-IN)



Esempi - Problemi di ricezione (SMTP-IN)

smtp(IN) log

•Se non c'è traccia della sessione a questo livello, neanche del tentativo di connessione, allora il problema di spedizione non è di Mdaemon

•Tracce di tutti i controlli della fase SMTP che potrebbero interrompere bruscamente la sessione facendo "perdere" il messaggio

•Tracce della parte in-line di alcuni controlli

- Antivirus
- Outbreak Protection
- Antispam (con punteggio euristico)

Approfondimenti nella KB

•**KB50567** - Come posso localizzare una mail attraverso i log di MDaemon?

•**KB50560** - Dove si possono recuperare informazioni sugli errori di tipo Winsock?

Esempi – SMTP(IN) log: messaggio rifiutato

Wed 2009-01-28 00:00:37: [2162:5] Session 2162; child 5; thread 141820
Wed 2009-01-28 00:00:37: [2162:5] Accepting SMTP connection from [**82.186.211.86**:34426]
Wed 2009-01-28 00:00:37: [2162:5] **Performing PTR lookup (86.211.186.82.IN-ADDR.ARPA)**
Wed 2009-01-28 00:00:37: [2162:5] * D=86.211.186.82.IN-ADDR.ARPA TTL=(5) PTR=[host86-211-static.186-82-b.business.telecomitalia.it]
Wed 2009-01-28 00:00:37: [2162:5] * Gathering A records...
Wed 2009-01-28 00:00:37: [2162:5] * D=host86-211-static.186-82-b.business.telecomitalia.it TTL=(720) A=[82.186.211.86]
Wed 2009-01-28 00:00:37: [2162:5] ---- End PTR results
Wed 2009-01-28 00:00:37: [2162:5] --> 220 mail.achab.it ESMTP MDaemon 9.6.6; Wed, 28 Jan 2009 00:00:37 +0100
Wed 2009-01-28 00:00:37: [2162:5] <-- **EHLO cdim.it**
Wed 2009-01-28 00:00:37: [2162:5] **Performing IP lookup (cdim.it)**
Wed 2009-01-28 00:00:37: [2162:5] *** Error: * Name server has no records of the requested type for that domain**
Wed 2009-01-28 00:00:37: [2162:5] ---- End IP lookup results
Wed 2009-01-28 00:00:37: [2162:5] --> 250-mail.achab.it Hello host86-211-static.186-82-b.business.telecomitalia.it, pleased to meet you
Wed 2009-01-28 00:00:37: [2162:5] --> 250-ETRN
Wed 2009-01-28 00:00:37: [2162:5] --> 250-AUTH=LOGIN
Wed 2009-01-28 00:00:37: [2162:5] --> 250-AUTH LOGIN CRAM-MD5
Wed 2009-01-28 00:00:37: [2162:5] --> 250-8BITMIME
Wed 2009-01-28 00:00:37: [2162:5] --> 250 SIZE 0
Wed 2009-01-28 00:00:37: [2162:5] <-- **MAIL From:<sales@achab.it> SIZE=2723**
Wed 2009-01-28 00:00:37: [2162:5] **Performing SPF lookup (achab.it / 82.186.211.86)**
Wed 2009-01-28 00:00:37: [2162:5] * Policy: v=spf1 mx ip4:213.140.23.64/27 -all
Wed 2009-01-28 00:00:37: [2162:5] * Evaluating mx: no match
Wed 2009-01-28 00:00:37: [2162:5] * Evaluating ip4:213.140.23.64/27: no match
Wed 2009-01-28 00:00:37: [2162:5] * Evaluating -all: match
Wed 2009-01-28 00:00:37: [2162:5] * **Result: fail**
Wed 2009-01-28 00:00:37: [2162:5] ---- End SPF results
Wed 2009-01-28 00:00:37: [2162:5] --> **550 failed to meet SPF requirements**
Wed 2009-01-28 00:00:37: [2162:5] SMTP session terminated (Bytes in/out: 52/285)
Wed 2009-01-28 00:00:37: ----------

Esempi – SMTP(IN) log: messaggio accettato (I)

- Wed 2009-01-28 00:01:09: ----------
- Wed 2009-01-28 00:01:09: [2189:4] Session 2189; child 4; thread 86836
- Wed 2009-01-28 00:01:08: [2189:4] **Accepting SMTP connection from [93.174.64.130:52038]**
- Wed 2009-01-28 00:01:08: [2189:4] **Performing PTR lookup (130.64.174.93.IN-ADDR.ARPA**)
- Wed 2009-01-28 00:01:08: [2189:4] * D=130.64.174.93.IN-ADDR.ARPA TTL=(731) PTR=[mx130.bouncemanager.it]
- Wed 2009-01-28 00:01:08: [2189:4] * Gathering A records...
- Wed 2009-01-28 00:01:08: [2189:4] * D=mx130.bouncemanager.it TTL=(762) A=[93.174.64.130]
- Wed 2009-01-28 00:01:08: [2189:4] ---- **End PTR results**
- Wed 2009-01-28 00:01:08: [2189:4] --> 220 mail.achab.it ESMTP MDaemon 9.6.6; Wed, 28 Jan 2009 00:01:08 +0100
- Wed 2009-01-28 00:01:08: [2189:4] <-- EHLO mx130.bouncemanager.it
- Wed 2009-01-28 00:01:08: [2189:4] **Performing IP lookup (mx130.bouncemanager.it)**
- Wed 2009-01-28 00:01:08: [2189:4] * D=mx130.bouncemanager.it TTL=(762) A=[93.174.64.130]
- Wed 2009-01-28 00:01:08: [2189:4] ---- **End IP lookup results**
- Wed 2009-01-28 00:01:08: [2189:4] --> 250-mail.achab.it Hello mx130.bouncemanager.it, pleased to meet you
- Wed 2009-01-28 00:01:08: [2189:4] --> 250-ETRN
- Wed 2009-01-28 00:01:08: [2189:4] --> 250-AUTH=LOGIN
- Wed 2009-01-28 00:01:08: [2189:4] --> 250-AUTH LOGIN CRAM-MD5
- Wed 2009-01-28 00:01:08: [2189:4] --> 250-8BITMIME
- Wed 2009-01-28 00:01:08: [2189:4] --> 250 SIZE 0
- Wed 2009-01-28 00:01:08: [2189:4] <-- **MAIL FROM:<ritorni@spotandweb.it> SIZE=7639**
- Wed 2009-01-28 00:01:08: [2189:4] **Performing IP lookup (spotandweb.it)**
- Wed 2009-01-28 00:01:08: [2189:4] * D=spotandweb.it TTL=(2) A=[62.149.128.163]
- Wed 2009-01-28 00:01:08: [2189:4] * D=spotandweb.it TTL=(2) A=[62.149.128.166]
- Wed 2009-01-28 00:01:08: [2189:4] * D=spotandweb.it TTL=(2) A=[62.149.128.72]
- Wed 2009-01-28 00:01:08: [2189:4] * D=spotandweb.it TTL=(2) A=[62.149.128.160]
- Wed 2009-01-28 00:01:08: [2189:4] * P=010 S=000 D=spotandweb.it TTL=(2) **MX=[mx.spotandweb.it] {62.149.128.74}**
- Wed 2009-01-28 00:01:08: [2189:4] ---- **End IP lookup results**

Esempi – SMTP(IN) log: messaggio accettato (II)

Wed 2009-01-28 00:01:08: [2189:4] **Performing SPF lookup (spotandweb.it / 93.174.64.130)**
Wed 2009-01-28 00:01:08: [2189:4] * **Result: none; no SPF record in DNS**
Wed 2009-01-28 00:01:08: [2189:4] ---- **End SPF results**
Wed 2009-01-28 00:01:08: [2189:4] --> 250 <ritorni@spotandweb.it>, Sender ok
Wed 2009-01-28 00:01:08: [2189:4] <-- **RCPT TO:<andrea.veca@achab.it>**
Wed 2009-01-28 00:01:08: [2189:4**] Performing DNS-BL lookup (93.174.64.130 - connecting IP)**
Wed 2009-01-28 00:01:08: [2189:4] * zen.spamhaus.org - passed
Wed 2009-01-28 00:01:08: [2189:4] ---- **End DNS-BL results**
Wed 2009-01-28 00:01:08: [2189:4] --> 250 <andrea.veca@achab.it>, Recipient ok
Wed 2009-01-28 00:01:08: [2189:4] <-- **DATA**
Wed 2009-01-28 00:01:08: [2189:4] Creating temp file (SMTP): d:\mdaemon\temp\md50000265653.tmp
Wed 2009-01-28 00:01:08: [2189:4] --> 354 Enter mail, end with <CRLF>.<CRLF>
Wed 2009-01-28 00:01:08: [2189:4] Message size: 7638 bytes
Wed 2009-01-28 00:01:09: [2189:4] **Performing DKIM lookup**
Wed 2009-01-28 00:01:09: [2189:4] * File: d:\mdaemon\temp\md50000265653.tmp
Wed 2009-01-28 00:01:09: [2189:4] * Message-ID: 200901280001080082.75.1150.852.73@SQL2.mailupid.com
Wed 2009-01-28 00:01:09: [2189:4] * **Result: neutral**
Wed 2009-01-28 00:01:09: [2189:4] ---- **End DKIM results**
Wed 2009-01-28 00:01:09: [2189:4] **Performing DomainKeys lookup (Sender: quotidiano@spotandweb.it)**
Wed 2009-01-28 00:01:09: [2189:4] * File: d:\mdaemon\temp\md50000265653.tmp
Wed 2009-01-28 00:01:09: [2189:4] * Message-ID: 200901280001080082.75.1150.852.73@SQL2.mailupid.com
Wed 2009-01-28 00:01:09: [2189:4] * Querying for policy: spotandweb.it
Wed 2009-01-28 00:01:09: [2189:4] * Querying: _domainkey.spotandweb.it ...
Wed 2009-01-28 00:01:09: [2189:4] * **DNS: * Name server reports domain name unknown**
Wed 2009-01-28 00:01:09: [2189:4] * **Result: neutral**
Wed 2009-01-28 00:01:09: [2189:4] ---- **End DomainKeys results**

Esempi – SMTP(IN) log: messaggio accettato (III)

Wed 2009-01-28 00:01:09: [2189:4] **Passing message through AntiVirus** (Size: 7638)...
Wed 2009-01-28 00:01:09: [2189:4] * **Message is clean** (no viruses found)
Wed 2009-01-28 00:01:09: [2189:4] ---- **End AntiVirus results**
Wed 2009-01-28 00:01:09: [2189:4] **Passing message through Outbreak Protection**...
Wed 2009-01-28 00:01:09: [2189:4] * Message-ID: 200901280001080082.75.1150.852.73@SQL2.mailupid.com
Wed 2009-01-28 00:01:09: [2189:4] * Reference-ID: str=0001.0A0B0205.497F9235.00C1:SCCE148,ss=1,fgs=0
Wed 2009-01-28 00:01:09: [2189:4] * **Virus result: 0 - Clean**
Wed 2009-01-28 00:01:09: [2189:4] * **Spam result: 1 - Clean**
Wed 2009-01-28 00:01:09: [2189:4] * **IWF result: 0 - Clean**
Wed 2009-01-28 00:01:09: [2189:4] ---- **End Outbreak Protection results**
Wed 2009-01-28 00:01:09: [2189:4] **Passing message through Spam Filter** (Size: 7638)...
Wed 2009-01-28 00:01:09: [2189:4] * 0.6 REPLY_TO_EMPTY Reply-To: is empty
Wed 2009-01-28 00:01:09: [2189:4] * 0.1 HTML_90_100 BODY: Message is 90% to 100% HTML
Wed 2009-01-28 00:01:09: [2189:4] * 0.0 HTML_MESSAGE BODY: HTML included in message
Wed 2009-01-28 00:01:09: [2189:4] * 1.6 BAYES_50 BODY: Bayesian spam probability is 40 to 60%
Wed 2009-01-28 00:01:09: [2189:4] * [score: 0.5017]
Wed 2009-01-28 00:01:09: [2189:4] * 0.0 MIME_HTML_ONLY BODY: Message only has text/html MIME parts
Wed 2009-01-28 00:01:09: [2189:4] * 0.0 FROM_EXCESS_QP From: quoted-printable encoded unnecessarily
Wed 2009-01-28 00:01:09: [2189:4] * 0.0 SUBJECT_EXCESS_QP Subject: quoted-printable encoded unnecessarily
Wed 2009-01-28 00:01:09: [2189:4] ---- **End SpamAssassin results**
Wed 2009-01-28 00:01:09: [2189:4] **Spam Filter score/req: 2.40/15.0**
Wed 2009-01-28 00:01:09: [2189:4] **Message creation successful: d:\mdaemon\inbound\md50003717885.msg**
Wed 2009-01-28 00:01:09: [2189:4] --> 250 Ok, message saved <Message-ID: 200901280001080082.75.1150.852.73@SQL2.mailupid.com>
Wed 2009-01-28 00:01:09: [2189:4] <-- **QUIT**
Wed 2009-01-28 00:01:09: [2189:4] --> 221 See ya in cyberspace
Wed 2009-01-28 00:01:09: [2189:4] SMTP session successful (Bytes in/out: 7759/455)
Wed 2009-01-28 00:01:09: ----------

Se il messaggio non è stato ricevuto allora il problema non si è verificato durante la sessione SMTP

Esempi – routing e content-filter log

Routing

Wed 2009-01-28 15:48:36: ----------

Wed 2009-01-28 15:48:50: Routing message (inbound queue): d:\mdaemon\inbound**md50003720800.msg**

Wed 2009-01-28 15:48:50: * From: subhasr@correo1.com; Recipient: corti-ncorti@corti.it; Size: 7356; Message: d:\mdaemon\localq**md50003102133.msg**

Wed 2009-01-28 15:48:50: * Subject: =?windows-1251?B?U29sdmluZyBBTEwgbG92ZSBtYWtpbmcgcHJvYmxlbXMgaW4gYSBtYXR0ZXIgb2YgZmV3IG1pbnV0ZXMu?=

Wed 2009-01-28 15:48:50: * Message-ID: 542a019dc00c$86831354$95a0b7af@correo1.com

Wed 2009-01-28 15:48:50: ----------

Content Filter

Wed 2009-01-28 15:48:35: ----------

Wed 2009-01-28 15:48:51: Content Filter processing d:\mdaemon\localq**md50003102133.msg**...

Wed 2009-01-28 15:48:51: * Message return-path: subhasr@correo1.com

Wed 2009-01-28 15:48:51: * Message from: subhasr@correo1.com

Wed 2009-01-28 15:48:51: * Message to: corti-ncorti@corti.it

Wed 2009-01-28 15:48:51: * Message subject: Solving ALL love making problems in a matter of few minutes.

Wed 2009-01-28 15:48:51: * Message ID: <542a019dc00c$86831354$95a0b7af@correo1.com>

Wed 2009-01-28 15:48:51: Start Content Filter results

Wed 2009-01-28 15:48:51: * Message matched rule: ASM_rule

Wed 2009-01-28 15:48:51: * Matched 1 of 30 active rules

Wed 2009-01-28 15:48:51: End of Content Filter results

Wed 2009-01-28 15:48:51: ----------

Routing

Wed 2009-01-28 15:48:50: ----------

Wed 2009-01-28 15:48:51: Routing message (local queue): d:\mdaemon\localq**pd50003102133.msg**

Wed 2009-01-28 15:48:51: * From: subhasr@correo1.com; Recipient: corti-ncorti@corti.it

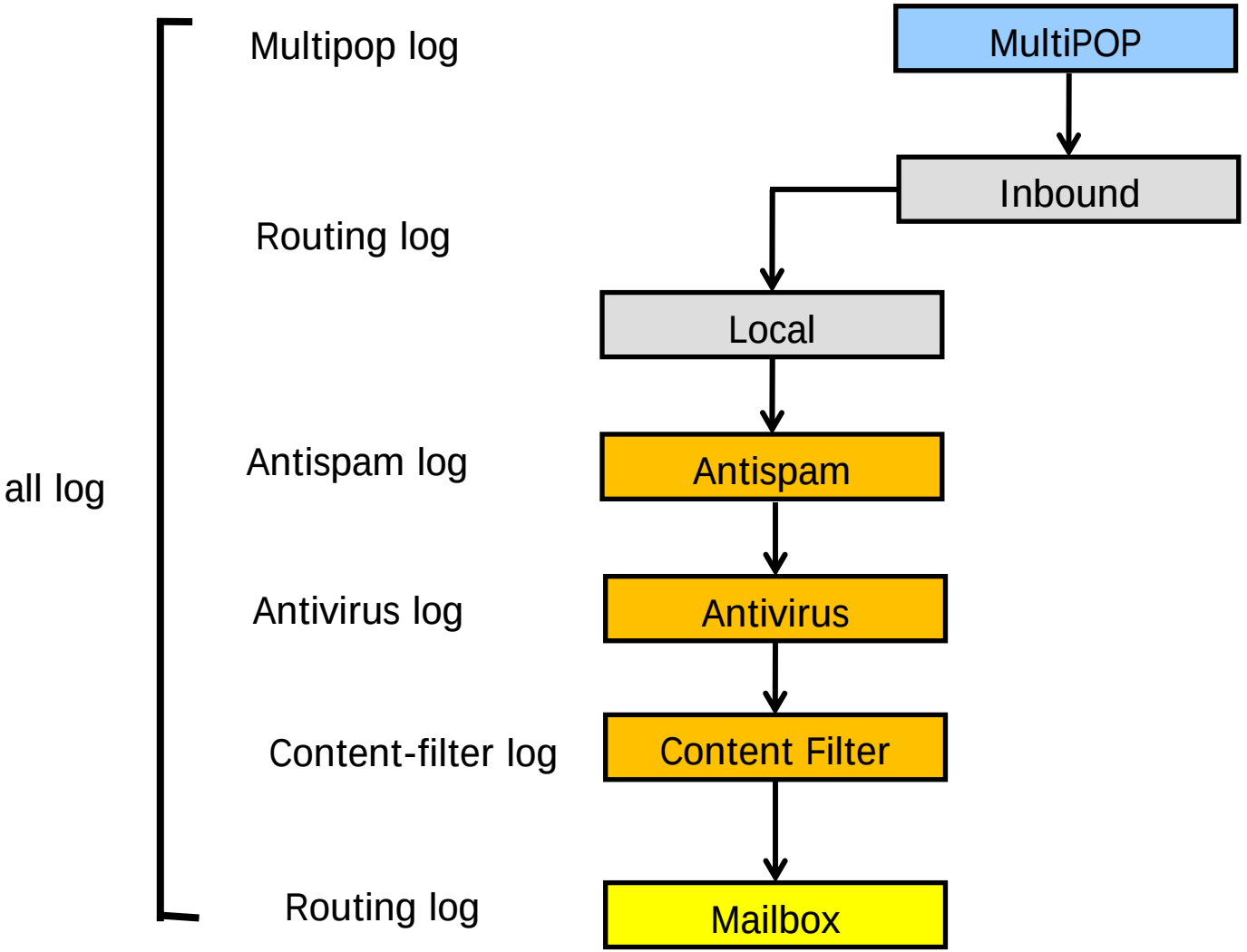
Wed 2009-01-28 15:48:51: * Subject: =?windows-1251?B?U29sdmluZyBBTEwgbG92ZSBtYWtpbmcgcHJvYmxlbXMgaW4gYSBtYXR0ZXIgb2YgZmV3IG1pbnV0ZXMu?=

Wed 2009-01-28 15:48:51: * Message-ID: <542a019dc00c$86831354$95a0b7af@correo1.com>

Wed 2009-01-28 15:48:51: * Size: 7420; Message: d:\mdaemon\users\corti.it\corti-ncorti**md50000790907.msg**

Wed 2009-01-28 15:48:51: ----------

Esempi - Problemi di ricezione (MultiPOP) (I)



Esempi - Problemi di ricezione (MultiPOP) (II)

- **Winsock Error 10060 The connection timed out.**
  Problemi di connessione con il server POP3 utilizzato nel Multipop
  Troubleshooting:
  - Testare con un ping se il server MDaemon riesce a raggiungere indirizzi esterni alla rete locale
  - Verificare con il comando telnet sulla porta 110 se il server POP3 del vostro provider risponde correttamente
  es.

  telnet pop3.libero.it 110
  +OK POP3 Server ready

- **Winsock Error 10053 Software caused a connection abort.**
  Il server POP3 è raggiungibile ma probabilmente ha delle restrizioni sul numero massimo di connessione aperte.
  Troubleshooting:
  - Ridurre il numero massimo di connessioni POP in uscita da MDaemon impostando il parametro **N. max di sessioni POP simultanee in uscita** presente in **Impostazioni --> Dominio principale --> Sessioni**

Esempi - Problemi di ricezione (MultiPOP) (III)

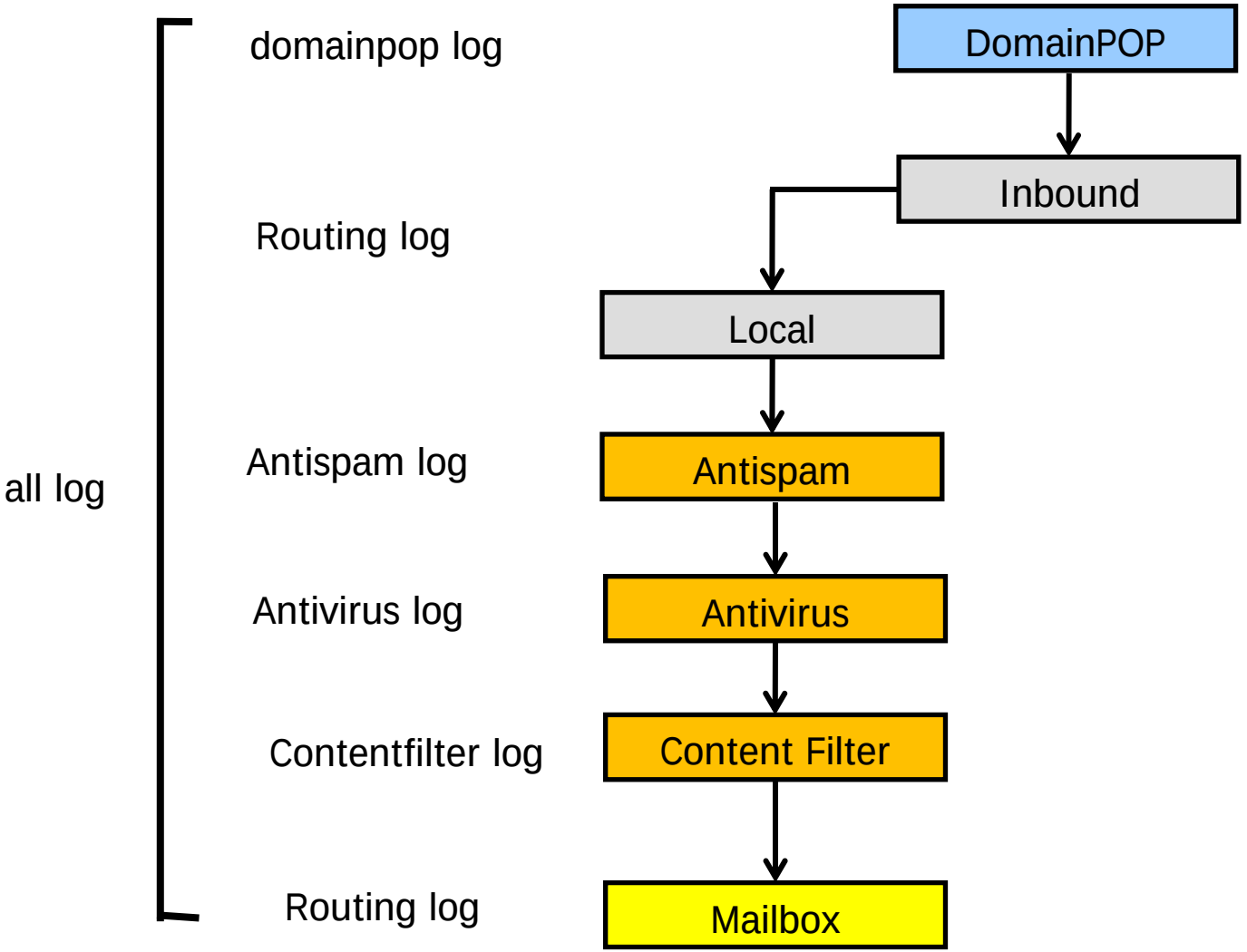
Wed 2009-01-28 12:34:04: Session 11; child 1
Wed 2009-01-28 12:34:02: **MultiPOP raccoglie la posta da (192.168.100.181) per (xxx)**
Wed 2009-01-28 12:34:02: La posta raccolta da MultiPOP NON viene rimossa dall'host remoto.
Wed 2009-01-28 12:34:02: **Attempting MultiPOP connection to [192.168.100.181:110]**
Wed 2009-01-28 12:34:02: Waiting for socket connection...
Wed 2009-01-28 12:34:02: * **Connection established (192.168.3.52:1088 -> 192.168.100.181:110)**
Wed 2009-01-28 12:34:02: Waiting for protocol to start...
Wed 2009-01-28 12:34:02: <-- +OK company.mail POP3 MDaemon ready using UNREGISTERED SOFTWARE 10.0.4 <MDAEMON-F200901281234.AA3401977MD8959@company.mail>
Wed 2009-01-28 12:34:02: --> **USER test1@company.mail**
Wed 2009-01-28 12:34:02: <-- +OK test1@company.mail... User ok
Wed 2009-01-28 12:34:02: --> **PASS ********
Wed 2009-01-28 12:34:02: <-- +OK test1@company.mail's mailbox has 4 total messages (22006 octets)
Wed 2009-01-28 12:34:02: --> **STAT**
Wed 2009-01-28 12:34:02: <-- +OK 4 22006
Wed 2009-01-28 12:34:02: --> **UIDL**
Wed 2009-01-28 12:34:02: 1 MD50000000017:MSG:1952:29980823:1427835392 - new message
Wed 2009-01-28 12:34:02: 2 MD50000000018:MSG:1870:29982855:1626618404 - new message
Wed 2009-01-28 12:34:02: 3 MD50000000019:MSG:17168:29982931:563739952 - new message
Wed 2009-01-28 12:34:02: 4 MD50000000020:MSG:1016:29982931:663742512 - new message
Wed 2009-01-28 12:34:02: --> .
Wed 2009-01-28 12:34:02: --> **NOOP**
Wed 2009-01-28 12:34:02: <-- +OK
Wed 2009-01-28 12:34:02: --> **LIST 1**
Wed 2009-01-28 12:34:03: <-- +OK 1 1952
Wed 2009-01-28 12:34:03: --> **RETR 1**
Wed 2009-01-28 12:34:03: <-- +OK 1952 octets
Wed 2009-01-28 12:34:03: Creating temp file (MPOP): c:\progra~1\mdaemon\queues\temp\14\md50000000001.tmp
Wed 2009-01-28 12:34:03: Transmission complete <c:\progra~1\mdaemon\queues\temp\14\md50000000001.tmp>
Wed 2009-01-28 12:34:03: **Creazione messaggio successful: c:\progra~1\mdaemon\queues\temp\14\md50000000001.tmp**

Esempi - Problemi di ricezione (MultiPOP) (IV)

Messaggi già scaricati

Wed 2009-01-28 12:34:04: ----------
Wed 2009-01-28 12:35:03: Session 12; child 1
Wed 2009-01-28 12:35:02: MultiPOP raccoglie la posta da (192.168.100.181) per (xxx)
Wed 2009-01-28 12:35:02: La posta raccolta da MultiPOP NON viene rimossa dall'host remoto.
Wed 2009-01-28 12:35:02: Attempting MultiPOP connection to [192.168.100.181:110]
Wed 2009-01-28 12:35:02: Waiting for socket connection...
Wed 2009-01-28 12:35:02: * Connection established (192.168.3.52:1094 -> 192.168.100.181:110)
Wed 2009-01-28 12:35:02: Waiting for protocol to start...
Wed 2009-01-28 12:35:02: <-- +OK company.mail POP3 MDaemon ready using UNREGISTERED SOFTWARE 10.0.4 <MDAEMON-F200901281235.AA3501964MD8228@company.mail>
Wed 2009-01-28 12:35:02: --> USER test1@company.mail
Wed 2009-01-28 12:35:02: <-- +OK test1@company.mail... User ok
Wed 2009-01-28 12:35:02: --> PASS ******
Wed 2009-01-28 12:35:02: <-- +OK test1@company.mail's mailbox has 4 total messages (22006 octets)
Wed 2009-01-28 12:35:02: --> STAT
Wed 2009-01-28 12:35:02: <-- +OK 4 22006
Wed 2009-01-28 12:35:02: --> **UIDL**
Wed 2009-01-28 12:35:02: **1 MD50000000017:MSG:1952:29980823:1427835392 - old message**
Wed 2009-01-28 12:35:02: **2 MD50000000018:MSG:1870:29982855:1626618404 - old message**
Wed 2009-01-28 12:35:02: **3 MD50000000019:MSG:17168:29982931:563739952 - old message**
Wed 2009-01-28 12:35:02: **4 MD50000000020:MSG:1016:29982931:663742512 - old message**
Wed 2009-01-28 12:35:02: --> .
Wed 2009-01-28 12:35:02: --> NOOP
Wed 2009-01-28 12:35:02: <-- +OK
Wed 2009-01-28 12:35:02: --> QUIT
Wed 2009-01-28 12:35:03: <-- +OK test1@company.mail company.mail POP3 Server signing off (4 messages left)
Wed 2009-01-28 12:35:03: POP3 session complete (Bytes in/out: 518/61)
Wed 2009-01-28 12:35:03: ----------

Esempi - Problemi di ricezione (DomainPOP) (I)



Esempi - Problemi di ricezione (DomainPOP) (II)

Fri 2008-11-07 08:15:31: Session 1120; child 1
Fri 2008-11-07 08:15:18: **Attempting DomainPOP connection to [78.4.212.37:110]**
Fri 2008-11-07 08:15:18: Waiting for socket connection...
Fri 2008-11-07 08:15:18: *** Connection established (127.0.0.1:3423 -> 78.4.212.37:110)**
Fri 2008-11-07 08:15:18: Waiting for protocol to start...
Fri 2008-11-07 08:15:18: <-- +OK Hello there.
Fri 2008-11-07 08:15:18: --> **USER dominio@artecimpianti.it**
Fri 2008-11-07 08:15:19: <-- +OK Password required.
Fri 2008-11-07 08:15:19: --> **PASS ********
Fri 2008-11-07 08:15:19: <-- +OK logged in.
Fri 2008-11-07 08:15:19: --> **STAT**
Fri 2008-11-07 08:15:19: <-- +OK 8 1391550
Fri 2008-11-07 08:15:19: --> **UIDL**
Fri 2008-11-07 08:15:19: **1 UID15555-1083567584 - new message**
Fri 2008-11-07 08:15:19: **2 UID15556-1083567584 - new message**
Fri 2008-11-07 08:15:19: **3 UID15557-1083567584 - new message**
Fri 2008-11-07 08:15:19: **4 UID15558-1083567584 - new message**
Fri 2008-11-07 08:15:19: **5 UID15559-1083567584 - new message**
Fri 2008-11-07 08:15:19: **6 UID15560-1083567584 - new message**
Fri 2008-11-07 08:15:19: **7 UID15561-1083567584 - new message**
Fri 2008-11-07 08:15:19: **8 UID15562-1083567584 - new message**
Fri 2008-11-07 08:15:19: --> .
Fri 2008-11-07 08:15:19: --> NOOP
Fri 2008-11-07 08:15:20: <-- +OK Yup.
Fri 2008-11-07 08:15:20: --> **LIST 1**
Fri 2008-11-07 08:15:20: <-- +OK 1 751874
Fri 2008-11-07 08:15:20: --> **RETR 1**
Fri 2008-11-07 08:15:20: <-- +OK 751874 octets follow.
Fri 2008-11-07 08:15:20: **Creating temp file (DPOP): c:\mdaemon\queues\temp\46\md50000000002.tmp**
Fri 2008-11-07 08:15:24: **Transmission complete <c:\mdaemon\queues\temp\46\md50000000002.tmp>**

Esempi - Problemi di ricezione (DomainPOP) (III)

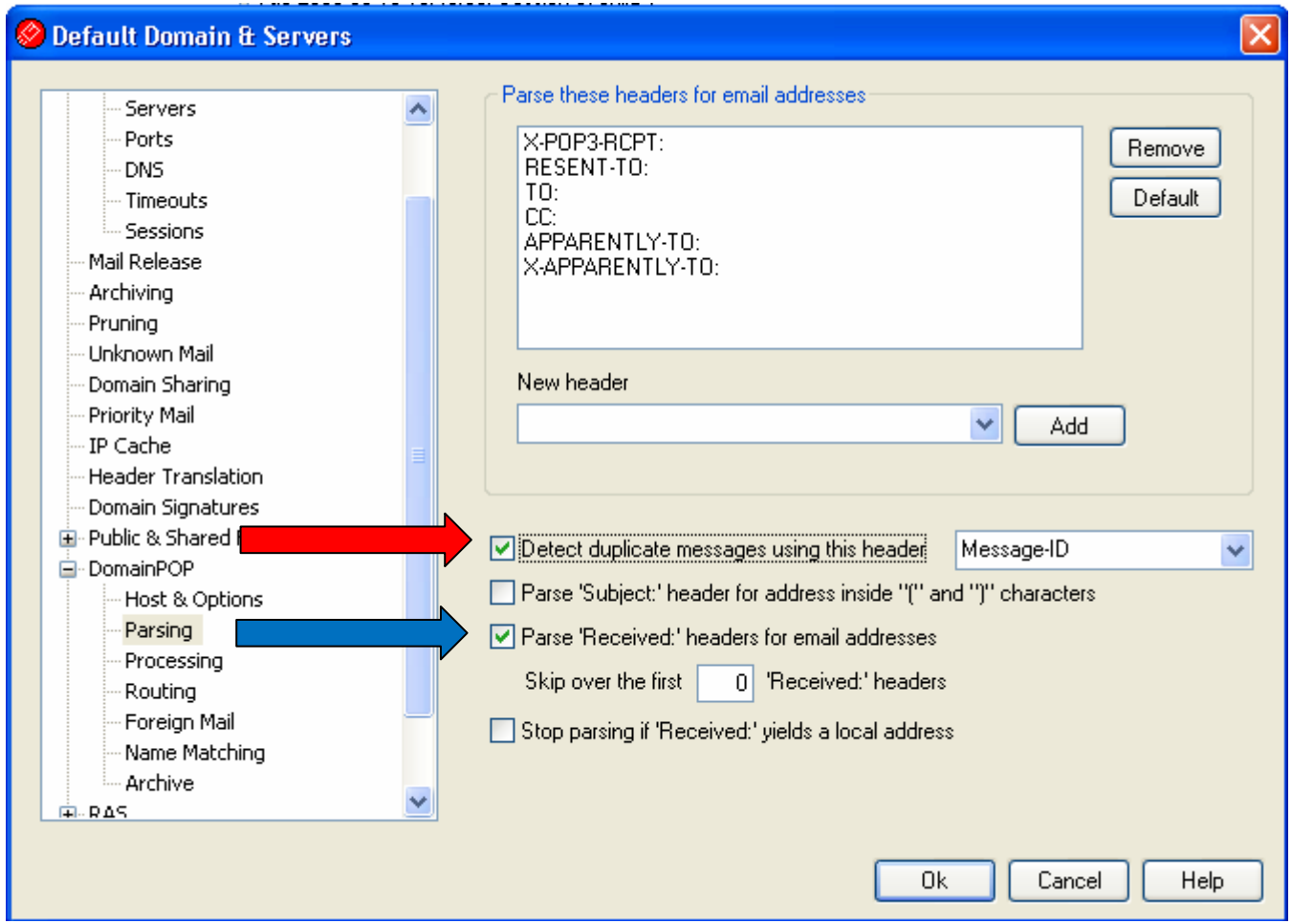
Fri 2008-11-07 08:15:24: **Indirizzo <dominio@artecimpianti.it> analizzato da intest. [RECEIVED:]**
Fri 2008-11-07 08:15:24: **Indirizzo <dominio@artecimpianti.it> analizzato da intestazione [RECEIVED:] (duplicata)**
Fri 2008-11-07 08:15:24: **Indirizzo <commerciale@artecimpianti.it> analizzato da intest. [RECEIVED:]**
Fri 2008-11-07 08:15:24: **Indirizzo <commerciale@artecimpianti.it> analizzato da intestazione [TO:] (duplicata)**
Fri 2008-11-07 08:15:24: **L'indirizzo <commerciale@artecimpianti.it> sopravvissuto all'analisi di tutti i DomainPOP, riceverà copia del messaggio**
Fri 2008-11-07 08:15:24: Creazione messaggio successful: c:\mdaemon\queues\temp\46\md50000000002.tmp
Fri 2008-11-07 08:15:24: --> **DELE 1**
Fri 2008-11-07 08:15:24: <-- +OK Deleted.
Fri 2008-11-07 08:15:24: --> **LIST 2**
Fri 2008-11-07 08:15:24: <-- +OK 2 110500
Fri 2008-11-07 08:15:24: --> **RETR 2**
Fri 2008-11-07 08:15:24: <-- +OK 110500 octets follow.
Fri 2008-11-07 08:15:24: Creating temp file (DPOP): c:\mdaemon\queues\temp\47\md50000000002.tmp
Fri 2008-11-07 08:15:25: Transmission complete <c:\mdaemon\queues\temp\47\md50000000002.tmp>

Altri log utili

- **System**: Visualizzazione del processo di inizializzazione che segnala eventuali problemi relativi alla configurazione o allo stato di MDaemon. Segnalati anche avvio o arresto dei vari server di Mdaemon
- **RAW**: In questa scheda vengono registrate le attività di posta RAW o generata dal sistema
- **Outlook Connector**: Vengono visualizzate le attività di Outlook Connector
- **WorldClient**: Vengono visualizzate le attività della sessione di WorldClient
- **SyncML**: Questa scheda riflette i dati contenuti nel file registro di SyncML.

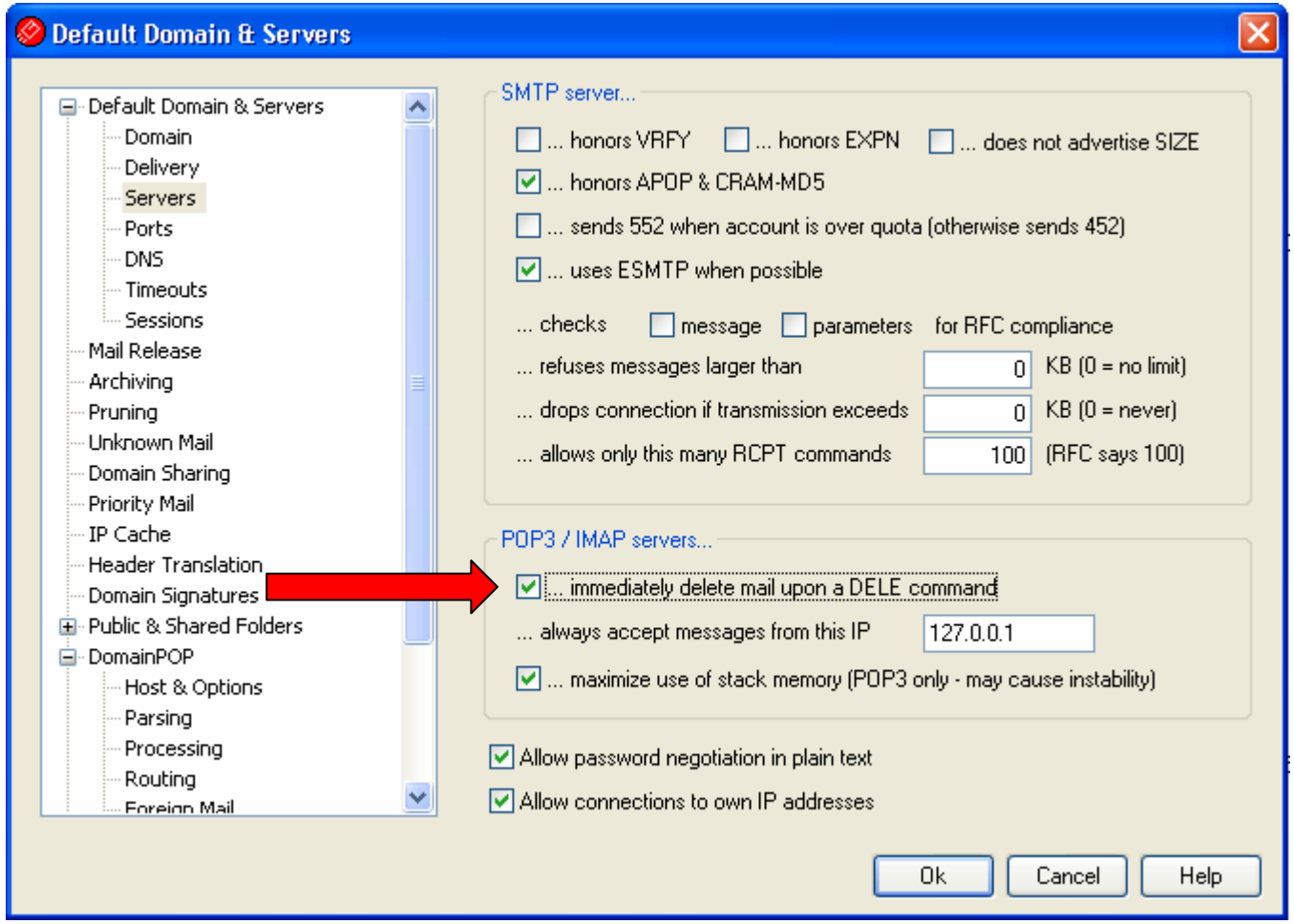
Esempi - Problemi di email ricevute duplicate

Ricezione via DomainPOP: può dipendere dalla configurazione.



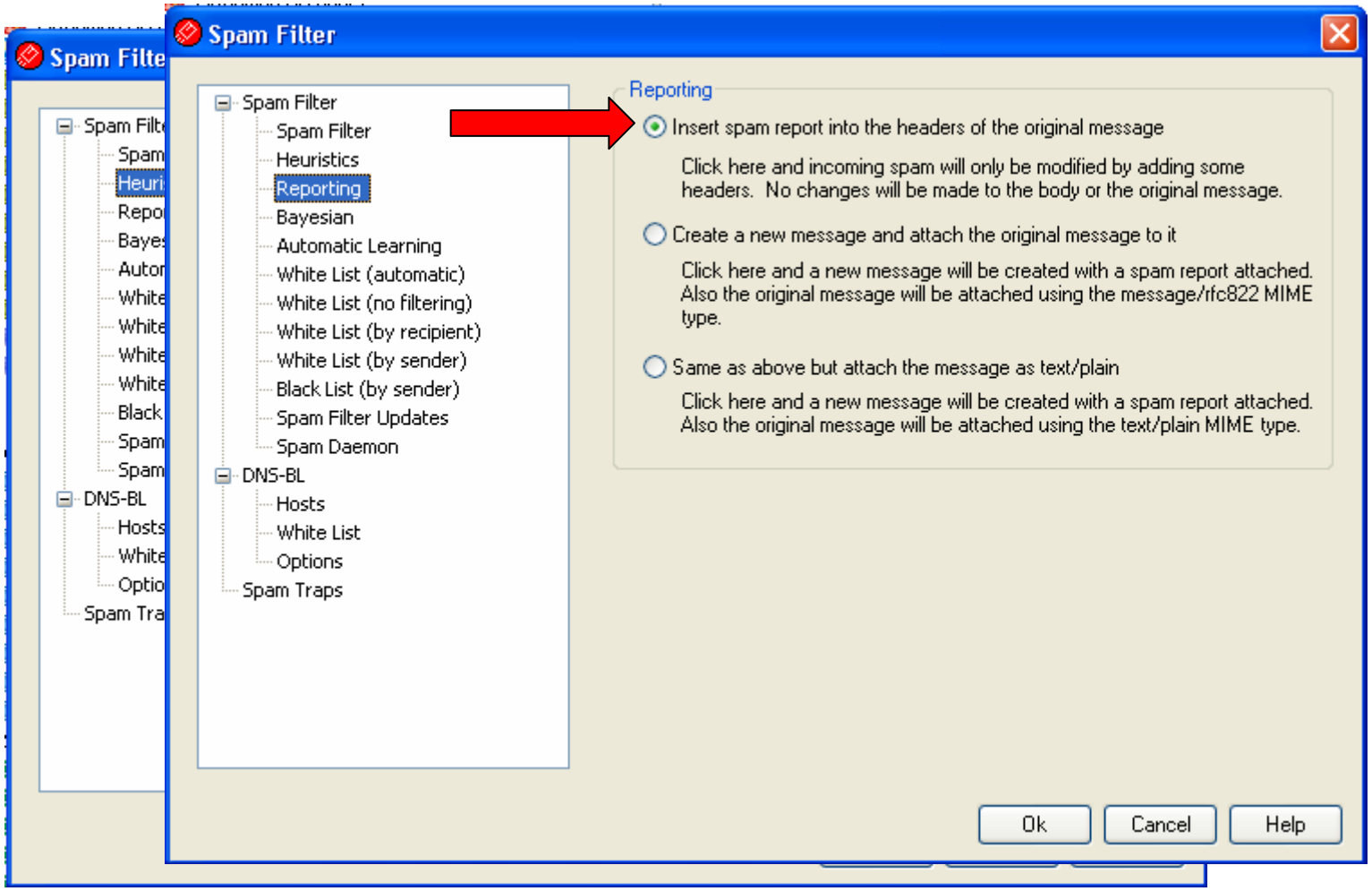
Esempi - Problemi di email ricevute duplicate

Ricezione via POP: può dipendere da sessioni incomplete



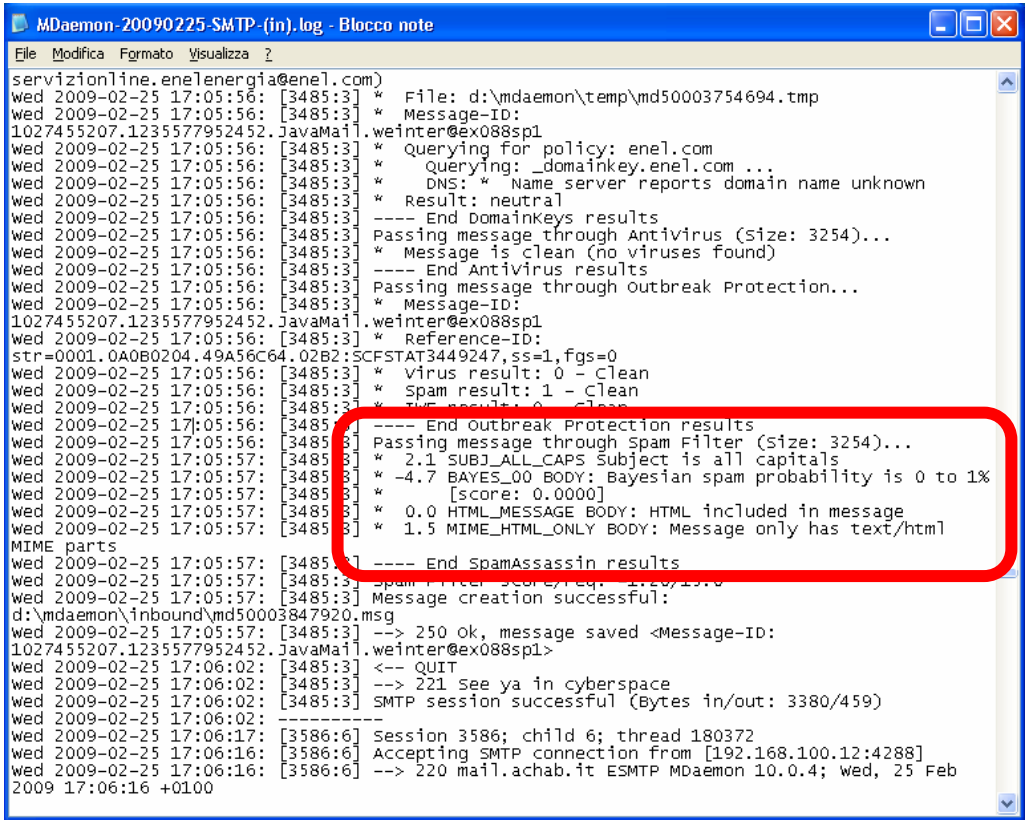
Esempi - Falsi positivi/negativi nello SPAM (I)

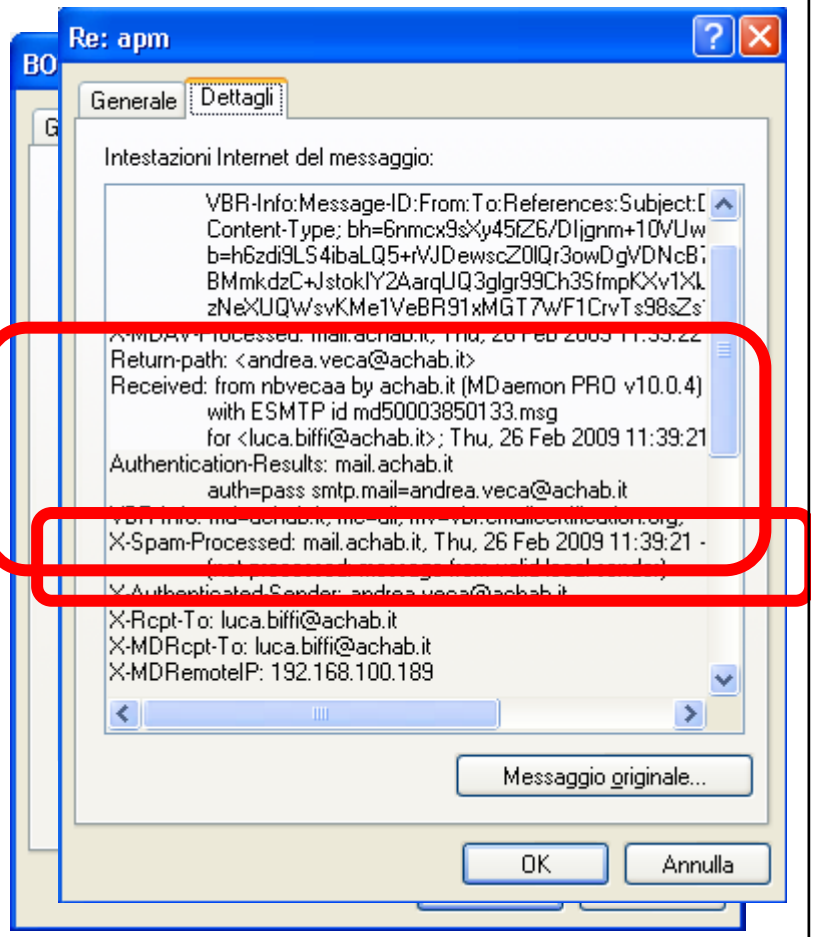
Security > Spam Filter


Spam Filter
Spam Filter
Heuristics
Reporting
Bayesian
Automatic Learning
White List (automatic)
White List (no filtering)
White List (by recipient)
White List (by sender)
Black List (by sender)
Spam Filter Updates
Spam Daemon
DNS-BL
Hosts
White List
Options
Spam Traps
Reporting
Insert spam report into the headers of the original message
Click here and incoming spam will only be modified by adding some headers. No changes will be made to the body or the original message.
Create a new message and attach the original message to it
Click here and a new message will be created with a spam report attached. Also the original message will be attached using the message/rfc822 MIME type.
Same as above but attach the message as text/plain
Click here and a new message will be created with a spam report attached. Also the original message will be attached using the text/plain MIME type.
Ok
Cancel
Help

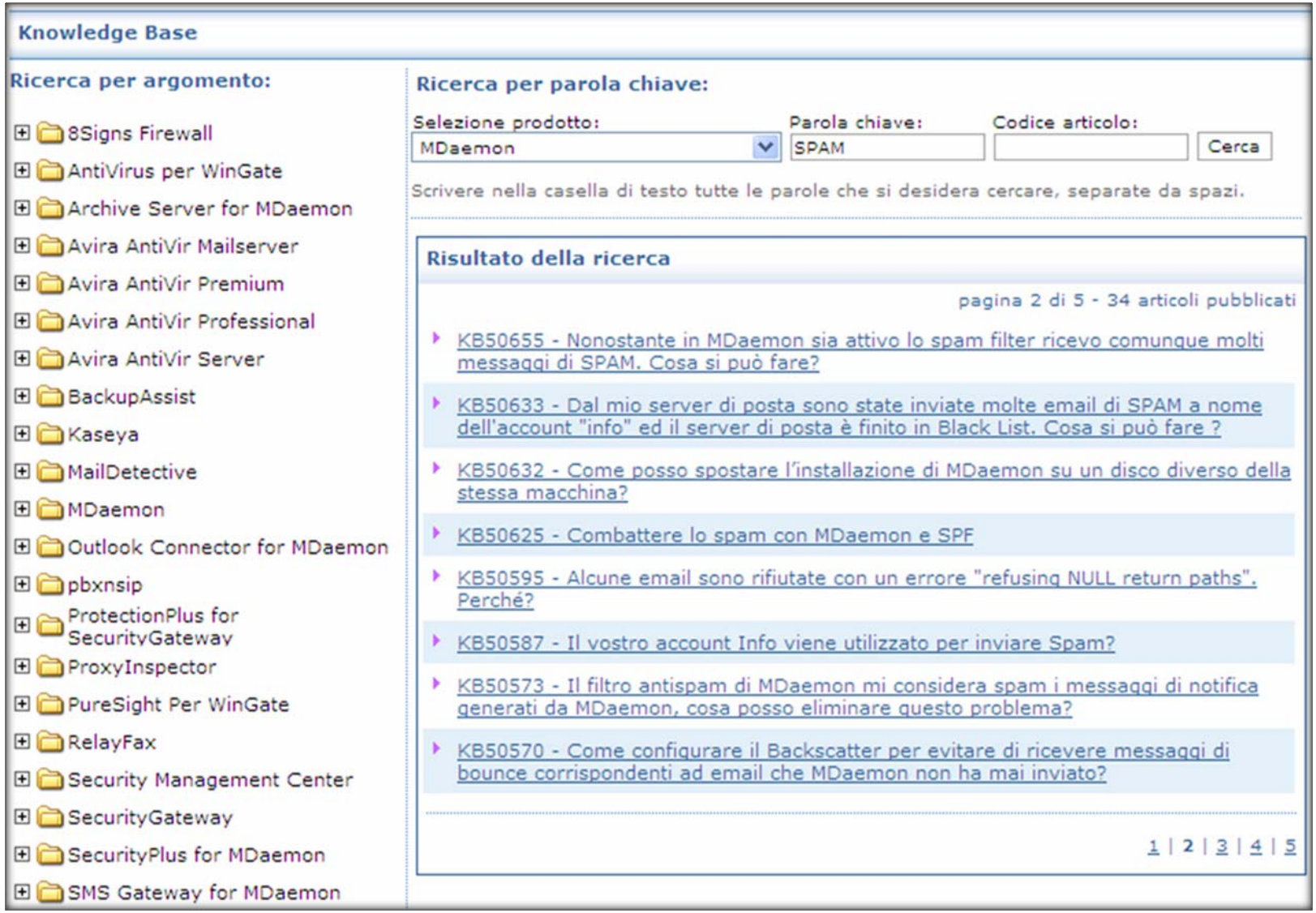
Esempi – Falsi positivi/negativi nello SPAM (II)

Analizzare i log (SMTP(IN), all) o l'header del messaggio


MDaemon-20090225-SMTP-(in).log - Blocco note
File Modifica Formato Visualizza ?
servizionline.enelenergia@enel.com)
wed 2009-02-25 17:05:56: [3485:3] * File: d:\mdaemon\temp\md50003754694.tmp
wed 2009-02-25 17:05:56: [3485:3] * Message-ID:
1027455207.1235577952452.JavaMail.weinter@ex088sp1
wed 2009-02-25 17:05:56: [3485:3] * Querying for policy: enel.com
wed 2009-02-25 17:05:56: [3485:3] * Querying: _domainkey.enel.com ...
wed 2009-02-25 17:05:56: [3485:3] * DNS: * Name server reports domain name unknown
wed 2009-02-25 17:05:56: [3485:3] * Result: neutral
wed 2009-02-25 17:05:56: [3485:3] ---- End DomainKeys results
wed 2009-02-25 17:05:56: [3485:3] Passing message through AntiVirus (Size: 3254)...
wed 2009-02-25 17:05:56: [3485:3] * Message is clean (no viruses found)
wed 2009-02-25 17:05:56: [3485:3] ---- End Antivirus results
wed 2009-02-25 17:05:56: [3485:3] Passing message through Outbreak Protection...
wed 2009-02-25 17:05:56: [3485:3] * Message-ID:
1027455207.1235577952452.JavaMail.weinter@ex088sp1
wed 2009-02-25 17:05:56: [3485:3] * Reference-ID:
str=0001.0A0B0204.49A56C64.02B2:SCFSTAT3449247,ss=1,fgs=0
wed 2009-02-25 17:05:56: [3485:3] * Virus result: 0 - Clean
wed 2009-02-25 17:05:56: [3485:3] * Spam result: 1 - Clean
wed 2009-02-25 17:05:56: [3485:3] * IWF result: 0 - Clean
wed 2009-02-25 17:05:56: [3485:3] ---- End Outbreak Protection results
wed 2009-02-25 17:05:56: [3485:3] Passing message through Spam Filter (Size: 3254)...
wed 2009-02-25 17:05:57: [3485:3] * 2.1 SUBJ_ALL_CAPS Subject is all capitals
wed 2009-02-25 17:05:57: [3485:3] * -4.7 BAYES_00 BODY: Bayesian spam probability is 0 to 1%
wed 2009-02-25 17:05:57: [3485:3] * [score: 0.0000]
wed 2009-02-25 17:05:57: [3485:3] * 0.0 HTML_MESSAGE BODY: HTML included in message
wed 2009-02-25 17:05:57: [3485:3] * 1.5 MIME_HTML_ONLY BODY: Message only has text/html
MIME parts
wed 2009-02-25 17:05:57: [3485:3] ---- End SpamAssassin results
wed 2009-02-25 17:05:57: [3485:3] Spam Filter score/req: 1.20/15.0
wed 2009-02-25 17:05:57: [3485:3] Message creation successful:
d:\mdaemon\inbound\md50003847920.msg
wed 2009-02-25 17:05:57: [3485:3] --> 250 Ok, message saved <Message-ID:
1027455207.1235577952452.JavaMail.weinter@ex088sp1>
wed 2009-02-25 17:06:02: [3485:3] <-- QUIT
wed 2009-02-25 17:06:02: [3485:3] --> 221 See ya in cyberspace
wed 2009-02-25 17:06:02: [3485:3] SMTP session successful (Bytes in/out: 3380/459)
wed 2009-02-25 17:06:02: ----------
wed 2009-02-25 17:06:17: [3586:6] Session 3586; child 6; thread 180372
wed 2009-02-25 17:06:16: [3586:6] Accepting SMTP connection from [192.168.100.12:4288]
wed 2009-02-25 17:06:16: [3586:6] --> 220 mail.achab.it ESMTP MDaemon 10.0.4; Wed, 25 Feb 2009 17:06:16 +0100



Esempi - Falsi positivi/negativi nello SPAM (III)


Knowledge Base
Ricerca per argomento:
8Signs Firewall
AntiVirus per WinGate
Archive Server for MDaemon
Avira AntiVir Mailserver
Avira AntiVir Premium
Avira AntiVir Professional
Avira AntiVir Server
BackupAssist
Kaseya
MailDetective
MDaemon
Outlook Connector for MDaemon
pbxnsip
ProtectionPlus for SecurityGateway
ProxyInspector
PureSight Per WinGate
RelayFax
Security Management Center
SecurityGateway
SecurityPlus for MDaemon
SMS Gateway for MDaemon
Ricerca per parola chiave:
Selezione prodotto:
MDaemon
Parola chiave:
SPAM
Codice articolo:
Cerca
Scrivere nella casella di testo tutte le parole che si desidera cercare, separate da spazi.
Risultato della ricerca
pagina 2 di 5 - 34 articoli pubblicati
KB50655 - Nonostante in MDaemon sia attivo lo spam filter ricevo comunque molti messaggi di SPAM. Cosa si può fare?
KB50633 - Dal mio server di posta sono state inviate molte email di SPAM a nome dell'account "info" ed il server di posta è finito in Black List. Cosa si può fare ?
KB50632 - Come posso spostare l'installazione di MDaemon su un disco diverso della stessa macchina?
KB50625 - Combattere lo spam con MDaemon e SPF
KB50595 - Alcune email sono rifiutate con un errore "refusing NULL return paths". Perché?
KB50587 - Il vostro account Info viene utilizzato per inviare Spam?
KB50573 - Il filtro antispam di MDaemon mi considera spam i messaggi di notifica generati da MDaemon, cosa posso eliminare questo problema?
KB50570 - Come configurare il Backscatter per evitare di ricevere messaggi di bounce corrispondenti ad email che MDaemon non ha mai inviato?
1 | 2 | 3 | 4 | 5

MDaemon®
Email Server
This program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program or any portion of it, may result in severe criminal and civil penalties, and will be prosecuted to the maximum extent possible under law.
Copyright 1996-2008 Alt-N Technologies, Ltd.
alt-n technologies

Grazie!

Claudio Panerai - Direttore Tecnico di Achab S.r.l.
claudio.panerai@achab.it

ACHAB
Quality Software Solutions